ABSTRACT OF THE DISCLOSURE

A device for and method of generating an uncorrelated pseudo-random bit sequence by first selecting a user-definable value K. Next, factoring K+1 into m prime factors $q_1,q_2,\ldots,q_m$, where $q_1,q_2,\ldots,q_m$ are ordered from smallest value q_1 to largest value q_m. Next, generating m pseudo-random sequences r_1, r_2,..., r_m, where each pseudo-random bit sequence r_i is uniformly distributed over a range (0,..., q_i-1), and where i = 1, 2, ..., m. Finally, generating the uncorrelated pseudo-random sequence as $R = r_1 + q_1r_2 + q_1 q_2 r_3 + \ldots + q_1 q_{2\ldots} q_{m-1}r_{m.}$